CITY AND COUNTY OF SAN FRANCISCO

DENNIS J. HERRERA
City Attorney

OFFICE OF THE CITY ATTORNEY

JOHN COTÉ
Press Secretary,
Communications Director

Direct Dial: (415) 554-4662
Email: john.cote@sfcityatty.org

May 17, 2019

VIA ELECTRONIC MAIL

Honorable Members of the Sunshine Ordinance Task Force
c/o: Clerk of the Board of Supervisors
Attn: Victor Young, Administrator
Room 244, City Hall
1 Dr. Carlton B. Goodlett Place
San Francisco CA 94102
victor.young@sfgov.org

Re: Sunshine Ordinance Task Force Complaint No. 19044
Anonymous (MuckRock News) v. Office of the City Attorney

Dear Honorable Task Force Members:

We write in response to the complaint filed by an anonymous person affiliated with MuckRock News, alleging that our office failed to respond to a request in a timely and/or complete manner. We received the request on April 22, 2019. It provided three email "message-Ids," and asked for either a native copy of the associated emails, or in the alternative a copy in PDF format, with the metadata from the native copy pasted into an attachment.

A message-Id is a unique tracking number for an email that is not visible in the body or header of the email, but is nonetheless available in the email's metadata. The term "metadata" refers to electronic data embedded in a document about the document itself. The amount of email metadata available for a particular email can vary greatly depending on the particulars of the email itself and the system(s) used to send and receive the email. Searching through metadata is a highly technical and specialized effort, and we do not believe we have ever received a request like this before.

If a requester already knows a particular email's message-Id, that may suggest that the requester already has access to the email in native form or to the metadata in which the message-Id is encoded. After investigating the matter with help from our information technology department, we were able to locate two responsive records: emails that MuckRock had exchanged with our office just one week prior, on April 18 and April 19. Although MuckRock presumably still had these emails, we produced the emails back to them, on April 24, in PDF format but without any further metadata. Upon receipt of the PDFs, MuckRock responded that it also wanted the metadata.

Our office generally does not produce metadata. State law does not provide authoritative guidance on whether metadata are subject to disclosure under the Public Records Act. Producing documents with metadata can subject the City to security risks and can lead to the inadvertent disclosure of privileged information. And the Public Records Act expressly does not require an agency to produce records in their electronic formats if it would jeopardize or compromise the

security or integrity of the original records, or of any proprietary software in which they are maintained. Cal. Govt. Code § 6253.9(f).

In this instance, we have elected to supplement our production, and have now given the requester the metadata we were able to find following a reasonable and diligent good faith search. *See* Exhibit A. To safeguard the security of our computer system, it is necessary for us to withhold certain portions of the metadata that describe unique identifiers for our individual computer terminals and computer servers and our security certificates and similar information. This information is highly sensitive, as disclosing it could allow a hacker to penetrate our system or enable a hacker to "spoof" our emails and insert themselves into attorney-client discussions or send unauthorized emails on our behalf. There is a real need for confidentiality that outweighs any interest the requester may have in accessing this information. *See* Cal. Evid. Code § 1040.

Our decision to disclose any metadata at all is limited to this specific case – the request covered only two emails, the emails were to and from MuckRock and therefore were not privileged, and we determined that disclosing these certain metadata excerpts would be unlikely to compromise the security or integrity of our system. We reserve our right to withhold metadata in response to future requests. Metadata may include a wide variety of information that the City Attorney's Office has a right, and in some cases a legal duty, to withhold from public view. For example, metadata may be used to reveal the history of how our office has edited a document or to whom within the City we have sent a draft, which is exempt from disclosure under the attorney-client privilege and work product privilege. Cal. Gov't Code § 6276.04; Cal. Evid. Code § 954; Cal. Code Civ. Proc. § 2018.030. Disclosing metadata could also reveal the identity of a confidential whistleblower, which is privileged. Cal. Evid. Code § 1041; Charter §§ C3.699-13(a), F1.107(c); C&GC Code §§ 4.120, 4.123. Finally, as with the metadata fields that we have redacted here, disclosure may also reveal sensitive information about the operation of the City's computer and communications system that a third party could use to hack into our system, or to otherwise undermine the integrity and security of our system.

A court is likely to conclude that the principles of reasonableness and cost containment that govern the disclosure of records under the Public Records Act and the Sunshine Ordinance allow the City to decline to produce metadata from electronic records. These principles would also allow the City to extend the normal deadlines for responding to a record request, to give the City time to investigate whether the metadata should be disclosed at all, and if so to perform any necessary redactions, particularly if the information requested was voluminous.

This position is consistent with our office's general position concerning the obligations of a City department with respect to metadata and the production of electronic records in PDF format, as stated in the Good Government Guide which is available on our website. *See* Exhibit B (excerpts). Because we have now complied with the request to search for and produce metadata, we respectfully ask that the complaint be dismissed.

Very truly yours,

DENNIS J. HERRERA
City Attorney

John Coté
Press Secretary, Communications Director

Coolbrith, Elizabeth (CAT)

From: Coolbrith, Elizabeth (CAT) on behalf of CityAttorney
Sent: Friday, May 17, 2019 3:20 PM
To: '72056-97339218@requests.muckrock.com'
Cc: CityAttorney
Subject: RE: California Public Records Act Request: Immediate Disclosure Request - Email Record Full Information
Attachments: 4-18-19 Email Received_Redacted.pdf

Dear Sir/Madam,

We have investigated your request further and have conducted a reasonable and diligent search and are able to supplement our production with the attached PDF. The PDF shows the headers and metadata associated with the email responsive to your request #s A3/A4. We have redacted some of the metadata based on the need to protect the security of our computer system. See Cal. Evid. Code section 1040. Also, please note that while we have agreed to produce some metadata excerpts in this instance, we reserve our right to revisit this approach in the future. Generally we do not disclose metadata at all, for the reasons stated to you in our prior responses.

Unfortunately, we were not able to locate headers/metadata for the emails responsive to your request #s A1/A2 and A5/A6. We have conducted a reasonable and diligent search for the information you asked for, but could not locate anything further.

As we have now complied with your request, we would respectfully ask that you withdraw your complaint to the Sunshine Ordinance Task Force as well as your petition to the Supervisor of Records.

Please send replies to cityattorney@sfcityatty.org

Sincerely,

Elizabeth A. Coolbrith
Paralegal
Office of City Attorney Dennis Herrera
(415) 554-4685 Direct
www.sfcityattorney.org
Find us on: Facebook Twitter Instagram

From: 72056-97339218@requests.muckrock.com <72056-97339218@requests.muckrock.com>
Sent: Wednesday, May 08, 2019 9:55 AM
To: CityAttorney <cityattorney@SFCITYATTY.ORG>
Cc: CityAttorney <cityattorney@SFCITYATTY.ORG>
Subject: RE: California Public Records Act Request: Immediate Disclosure Request - Email Record Full Information

San Francisco City Attorney
PRA Office

Room 234
1 Doctor Carlton B Goodlett Place
SF, CA 94102

May 8, 2019

This is a follow up to a previous request:

Your PDFs include From, To, Subject, Sent, Attachments, and Body of the emails. You have withheld certain portions of the email records, including but not limited to:
- Header: X-Envelope-From
- Header: Received
- Header: Thread-Topic
- Header: X-Originating-Ip
- Header: Thread-Index
- Header: Sender
- Header: X-Originatororg

Please provide a statutory justification for such withholding, and the name and title of the official responsible for that withholding, per CPRA.

Note that all of your responses (including disclosed records) may be automatically and instantly available to the public on the MuckRock.com service used to issue this request (though I am not a MuckRock representative).

Filed via MuckRock.com
E-mail (Preferred): 72056-97339218@requests.muckrock.com
Upload documents directly:
https://accounts.muckrock.com/accounts/login/?next=https%3A%2F%2Fwww.muckrock.com%2Faccounts%2Flogin%2F%3Fnext%3D%252Faccounts%252Fagency_login%252Fsan-francisco-city-attorney-797%252Fimmediate-disclosure-request-email-record-full-information-72056%252F%253Femail%253Dcityattorney%252540sfcityatty.org&url_auth_token=AAAuFBaWTyfyRXNxLh3MkFOGTxo%3A1hOPqN%3A7oronmiVFTUFdl0TsdhK9kZpwVk
Is this email coming to the wrong contact? Something else wrong? Use the above link to let us know.

For mailed responses, please address (see note):
MuckRock News
DEPT MR 72056
411A Highland Ave
Somerville, MA 02144-2516

PLEASE NOTE: This request is not filed by a MuckRock staff member, but is being sent through MuckRock by the above in order to better track, share, and manage public records requests. Also note that improperly addressed (i.e., with the requester's name rather than "MuckRock News" and the department number) requests might be returned as undeliverable.

On May 8, 2019:
Hello,

We already completed our response to your request on April 24, 2019. We do not intend to produce anything further in response to your request.

Please send replies to cityattorney@sfcityatty.org<mailto:cityattorney@sfcityatty.org>

Sincerely,

[cid:image002.jpg@01D50583.20D9FFB0]Elizabeth A. Coolbrith
Paralegal
Office of City Attorney Dennis Herrera
(415) 554-4685 Direct
www.sfcityattorney.org
Find us on: Facebook<https://www.facebook.com/sfcityattorney/>
Twitter<https://twitter.com/SFCityAttorney> Instagram<https://www.instagram.com/sfcityattorney/>

On April 24, 2019:
Thank you. As we noted in our initial request, we requested the entire email message, which contains numerous other headers in addition to those you have provided so far.
We do not see any statutory justification cited for withholding that portion of the public record. Please do provide the entire message with all headers (except those statutorily excluded from disclosure).

On April 24, 2019:
Dear Sir/Madam,

The attached two emails are responsive to portions A3/A4, and A5/A6 of your request below. We have conducted a reasonable and diligent search and did not locate any further responsive documents.

In addition, please note that we already responded to portion B of your request, on 4/22/2019.

If you have further questions or need anything additional, please feel free to reach out to us at the below contact information.

Please send replies to cityattorney@sfcityatty.org<mailto:cityattorney@sfcityatty.org>

Sincerely,

[cid:image002.jpg@01D4FA8E.F0958DA0]Elizabeth A. Coolbrith
Paralegal
Office of City Attorney Dennis Herrera
(415) 554-4685 Direct
www.sfcityattorney.org
Find us on: Facebook<https://www.facebook.com/sfcityattorney/>
Twitter<https://twitter.com/SFCityAttorney> Instagram<https://www.instagram.com/sfcityattorney/>

On April 23, 2019:
Hello,

I am writing in response to part A of your below request.

Your request was sent as an "Immediate Disclosure Request" under San Francisco Administrative Code Section 67.25(a). But to qualify under that section, the request must be "simple, routine and readily answerable." The Sunshine Ordinance requires shorter response times in those situations where a department is able to quickly locate and produce the requested records. In order to respond to your request, this office will need to conduct a review of our electronic files to find responsive records. For this reason, we are not treating your request as one appropriately filed as an "immediate disclosure" request, but as one which is subject to the normally applicable 10-day response time, which will be May 2, 2019. However, we will endeavor to fulfill your request as soon as possible.

Please send replies to cityattorney@sfcityatty.org<mailto:cityattorney@sfcityatty.org>

Sincerely,

[cid:image002.jpg@01D4F9EE.FD8B8960]Elizabeth A. Coolbrith
Paralegal
Office of City Attorney Dennis Herrera
(415) 554-4685 Direct
www.sfcityattorney.org
Find us on: Facebook<https://www.facebook.com/sfcityattorney/>
Twitter<https://twitter.com/SFCityAttorney> Instagram<https://www.instagram.com/sfcityattorney/>

On April 22, 2019:
Message-Ids uniquely identify e-mail messages in your email servers.
From the headers of your most recent email, it appears your office uses Microsoft Outlook and/or Microsoft Exchange - therefore, your IT department/contractor should be able to retrieve e-mail records directly from your server using the Message-Ids we have provided.

On April 20, 2019:
This is an Immediate Disclosure Request under the San Francisco Sunshine Ordinance.

We request under the San Francisco Sunshine Ordinance (Ordinance) and the California Public Records Act (CPRA):

"A. an electronic copy, in the original electronic format, with all e-mail headers, metadata, attachments, appendices, exhibits, and inline images, except those explicitly exempted by the Ordinance, of:

A1. the e-mail message with Message-Id:
20190418173050.839.30844@f720c6d2-4be2-4478-af65-b9b764b16768.prvt.dyno.rt.heroku.com

A2. the e-mail message with Message-Id:
<20190418173050.839.30844@f720c6d2-4be2-4478-af65-b9b764b16768.prvt.dyno.rt.heroku.com>

A3. the e-mail message with Message-Id:
20190418173050.1.2B43534B4544D903@requests.muckrock.com

A4. the e-mail message with Message-Id:
<20190418173050.1.2B43534B4544D903@requests.muckrock.com>

A5. the e-mail message with Message-Id:
<DM5PR09MB1497363CAABBE6806E68810F80260@DM5PR09MB1497.namprd09.prod.outlook.com>

A6. the e-mail message with Message-Id:
DM5PR09MB1497363CAABBE6806E68810F80260@DM5PR09MB1497.namprd09.prod.outlook.com

B. an electronic copy of your internal public records policies/manuals/instructions/guidelines for the public and/or your own employees"

Message-Id's should uniquely identify a particular email on your email servers/services. These may be emails the City sent or received.

We remind you of your obligations to provide electronic records in the original format you hold them in. Therefore, e-mails exported in the .eml or .msg format with all non-exempt headers, metadata, attachments, etc. are best.

However, if you choose to convert emails, for example, to PDF or printed format, to easily redact them, you must ensure that you have preserved the full content of the original email record (as specified in request "A"), which contains many detailed headers beyond the generally used From/To/Subject/Sent/etc. If you instead provide PDFs or printed emails with only a few of the headers or lacking attachments/images, and therefore withhold the other headers/attachments without justification, you may be in violation of SF Admin Code 67.26, 67.27, Govt Code 6253(a), 6253.9, and/or 6255, and we may challenge your decision.

Note that all of your responses (including disclosed records) may be automatically and instantly available to the public on the MuckRock.com service used to issue this request (though I am not a MuckRock representative).

Please provide only those copies of records available without any fees. If you determine certain records would require fees, please instead provide the required notice of which of those records are available and non-exempt for inspection in-person if we so choose.

I look forward to your immediate disclosure.

Sincerely,
Anonymous

Filed via MuckRock.com
E-mail (Preferred): 72056-97339218@requests.muckrock.com
Upload documents directly:
https://accounts.muckrock.com/accounts/login/?next=https%3A%2F%2Fwww.muckrock.com%2Faccounts%2Flogin%2F%3Fnext%3D%252Faccounts%252Fagency_login%252Fsan-francisco-city-attorney-797%252Fimmediate-disclosure-request-email-record-full-information-72056%252F%253Femail%253Dcityattorney%252540sfcityatty.org&url_auth_token=AAAuFBaWTyfyRXNxLh3MkFOGTxo%3A1hOPqN%3A7oronmiVFTUFdl0TsdhK9kZpwVk
Is this email coming to the wrong contact? Something else wrong? Use the above link to let us know.

For mailed responses, please address (see note):
MuckRock News
DEPT MR 72056

411A Highland Ave
Somerville, MA 02144-2516

PLEASE NOTE: This request is not filed by a MuckRock staff member, but is being sent through MuckRock by the above in order to better track, share, and manage public records requests. Also note that improperly addressed (i.e., with the requester's name rather than "MuckRock News" and the department number) requests might be returned as undeliverable.

[redacted]

[redacted]

Date: Thu, 18 Apr 2019 17:30:50 +0000
Sender: 71969-51399120@requests.muckrock.com
Message-Id: <20190418173050.1.2B43534B4544D903@requests.muckrock.com>
[redacted]
To: cityattorney@sfcityatty.org
From: 71969-51399120@requests.muckrock.com
Subject: California Public Records Act Request: Immediate Disclosure Request
 - PRA Opinions
Mime-Version: 1.0
Content-Type: multipart/mixed; boundary="b2e1fbcebbd64db587dfc7e9a4eeaf40"
Return-Path:
 bounce+5bea6f.556-cityattorney=sfcityatty.org@requests.muckrock.com
[redacted]

[redacted]

X-MS-Exchange-Organization-MessageDirectionality: Incoming

[redacted]

X-MS-PublicTrafficType: Email

[redacted]

[redacted]

Good Government Guide

An Overview of the Laws Governing
the Conduct of Public Officials

PAGES 1-122 LAST UPDATED FEBRUARY 2019
PAGES 122-193 LAST UPDATED SEPTEMBER 2014

Dennis J. Herrera
City Attorney of San Francisco

The Public Records Act imposes additional requirements about information that is in an electronic format. Cal. Govt. Code § 6253.9. As a general rule, the Act requires a department to make the information available in any electronic format in which it holds the information, and to make a copy of an electronic record available in the format requested if the department has used that format to create copies for its own use or for other agencies. Cal. Govt. Code §§ 6253.9(a)(1), (2). But these provisions do not require a department to reconstruct a record in an electronic format if the record is no longer available electronically or create it in a format it has not used. Cal. Govt. Code § 6253.9(c). However, the text of the Sunshine Ordinance on these issues is not clear, so the safer legal course is to make electronic records available in the format requested if that can be easily accomplished without requiring the department to reprogram a computer. This general approach is subject to limitations, discussed below, regarding metadata and easily manipulated formats.

The Sunshine Ordinance does not require a department to program or reprogram a computer to respond to a public records request. Admin. Code § 67.21(l). But, as explained below, the Public Records Act does. In this respect, the rule that a department has no duty to create a record has evolved in the electronic age: where information exists in electronic form, a department must engage in data compilation, extraction, or programming to produce the electronic record, provided the requester is willing to pay for the cost of production which includes the programming or reprogramming of the computer. Cal. Govt. Code § 6253.9(b)(2). In similar fashion, a department must produce an electronic copy of a record that it ordinarily produces at regularly scheduled intervals. Cal. Govt. Code § 6253.9(b)(1).

ii. Portable Document Format, or PDF

To facilitate accessibility and ease of use, many City departments provide their electronic records to the public as PDF files. PDF, which stands for "Portable Document Format," is a file format created by Adobe Systems in the early 1990s to facilitate the exchange of electronic documents across multiple operating systems, and without requiring the purchase of specific software or hardware. PDF is now an open standard, meaning it is available without charge, is non-proprietary, and can be accommodated by different software. The advantages of providing records in this format are that:

- PDF is a free, open format.
- PDF records are viewable and printable on any computer platform.
- PDF records typically look like the original records and thus preserve the integrity of the original information.
- PDF records can enable full-text searches to locate words and terms features in PDF documents that are saved in electronic format.
- PDF records work with assistive technologies to make the information available to persons with disabilities.

iii. Metadata

Sometimes a requester seeks a record in its original electronic format, which likely involves proprietary software, such as Microsoft Word or Excel. In such instances, the electronic

document will usually contain embedded, hidden information known as "metadata." Metadata may include information such as when the document was originally created; the document's authors and editors; comments shared among co-authors and editors; and tracked changes in versions of the document before its completion. These metadata may not be readily apparent in the final document, but may nonetheless be fully available to the recipient were the document provided in its native file format. Depending on the nature of the record requested, some or all of the metadata it contains may be properly exempt from disclosure. In still other instances – including comments that may contain legal advice, medical, personnel or otherwise private information – the disclosure of metadata might be restricted or actually prohibited by law.

While case law does not provide authoritative guidance on legal questions relating to public disclosure of metadata, and while technologies continue to evolve, there is no evidence that either the Public Records Act or the Sunshine Ordinance was intended to require public entities to search, and then review and possibly redact, metadata in electronic records. Neither is there an apparent legislative intent to require government agencies to produce records in their electronic formats if their release would jeopardize or compromise the security or integrity of the original records, or of any proprietary software in which they are maintained. Cal. Govt. Code § 6253.9(f).

At the same time, department personnel should consider the usability of public information provided to requesters in responding to public records requests. In asking for a public record in a native file format like Microsoft Excel, for example, a requester may simply be seeking a format that will enable searching, querying, manipulating and summarizing public information in a manner that is far easier than if the record were provided in a scanned PDF or on a printed page. In some instances, the very same technology innovations that can present difficult public records questions may help resolve these issues through conversion to file formats that both meet the requester's needs and avoid problems with unauthorized disclosure of metadata. Departments seeking further advice on these issues or other issues pertaining to metadata, including where a public records request specifically seeks metadata, should consult with their information technology staff and with the City Attorney's Office.

A Board of Supervisors' policy directs its clerk to provide responsive records in the original format when the requester so requests. Other departments may wish to consider their own policy options in light of the possible risks of unintended or impermissible disclosure of metadata in documents specific to their own department's functions.

iv. Information on personal communications devices

Communications relating to the City's business that a public employee or official sends or receives on personal electronic devices such as cell phones and personal computers are subject to disclosure as public records. The key criteria for determining whether such a communication is a public record are the content and context of the record, including the purpose of the communication and the sender(s) and intended recipient(s); whether it concerns City business; and whether a City official or employee has received or created it in the performance of work duties, even if not required or solicited. For more information on

The New York Times

A Cyberattack Hobbles Atlanta, and Security Experts Shudder

By Alan Blinder and Nicole Perlroth

March 27, 2018

ATLANTA — The City of Atlanta's 8,000 employees got the word on Tuesday that they had been waiting for: It was O.K. to turn their computers on.

But as the city government's desktops, hard drives and printers flickered back to life for the first time in five days, residents still could not pay their traffic tickets or water bills online, or report potholes or graffiti on a city website. Travelers at the world's busiest airport still could not use the free Wi-Fi.

Atlanta's municipal government has been brought to its knees since Thursday morning by a ransomware attack — one of the most sustained and consequential cyberattacks ever mounted against a major American city.

The digital extortion aimed at Atlanta, which security experts have linked to a shadowy hacking crew known for its careful selection of targets, laid bare once again the vulnerabilities of governments as they rely on computer networks for day-to-day operations. In a ransomware attack, malicious software cripples a victim's computer or network and blocks access to important data until a ransom is paid to unlock it.

"We are dealing with a hostage situation," Mayor Keisha Lance Bottoms said this week.

The assault on Atlanta, the core of a metropolitan area of about six million people, represented a serious escalation from other recent cyberattacks on American cities, like one last year in Dallas where hackers gained the ability to set off tornado sirens in the middle of the night.

Part of what makes the attack on Atlanta so pernicious are the criminals behind it: A group that locks up its victims' files with encryption, temporarily changes their file names to "I'm sorry" and gives the victims a week to pay up before the files are made permanently inaccessible.

Threat researchers at Dell SecureWorks, the Atlanta-based security firm helping the city respond to the ransomware attack, identified the assailants as the SamSam hacking crew, one of the more prevalent and meticulous of the dozens of active ransomware attack groups. The SamSam group is known for choosing targets that are the most likely to accede to its high ransom demands — typically the Bitcoin equivalent of about $50,000 — and for finding and locking up the victims' most valuable data.

In Atlanta, where officials said the ransom demand amounted to about $51,000, the group left parts of the city's network tied in knots. Some major systems were not affected, including those for 911 calls and control of wastewater treatment. But other arms of city government have been scrambled for days.

The Atlanta Municipal Court has been unable to validate warrants. Police officers have been writing reports by hand. The city has stopped taking employment applications.

Atlanta officials have disclosed few details about the episode or how it happened. They have urged vigilance and tried to reassure employees and residents that their personal information was not believed to have been compromised.

Dell SecureWorks and Cisco Security, which are still working to restore the city's systems, declined to comment on the attacks, citing client confidentiality.

Ms. Bottoms, the mayor, has not said whether the city would pay the ransom.

The SamSam group has been one of the more successful ransomware rings, experts said. It is believed to have extorted more than $1 million from some 30 target organizations in 2018 alone.

It is not ideal to pay up, but in most cases, SamSam's victims have said that they can more easily afford the $50,000 or so in ransom than the time and cost of restoring their locked data and compromised systems. In the past year, the group has taken to attacking hospitals, police departments and universities — targets with money but without the luxury of going off-line for days or weeks for restoration work.

Investigators are not certain who the SamSam hackers are. Judging from the poor English in the group's ransom notes, security researchers believe they are probably not native English speakers. But they cannot say for sure whether SamSam is a single group of cybercriminals or a loose hacking collective.

Ransomware emerged in Eastern Europe in 2009, when cybercriminals started using malicious code to lock up unsuspecting users' machines and then demanding 100 euros or similar sums to unlock them again. Over the past decade, dozens of online cybercriminal outfits — and even some nation states, including North Korea and Russia — have taken up similar tactics on a larger scale, inflicting digital paralysis on victims and demanding increasing amounts of money.

Cybersecurity experts estimate that criminals made more than $1 billion from ransomware in 2016, according to the F.B.I. Then, last May, came the largest ransomware assault recorded so far: North Korean hackers went after tens of thousands of victims in more than 70 countries around the world, forcing Britain's public health system to reject patients, paralyzing computers at Russia's Interior Ministry, at FedEx in the United States, and at shipping lines and telecommunications companies across Europe.

A month later, Russian state hackers deployed similar ransomware to paralyze computers in Ukraine on the eve of the country's independence day. That attack shut down automated teller machines in Kiev, froze government agencies and even forced workers at the Chernobyl nuclear power plant to monitor radiation levels manually. Collateral damage from that attack affected computers at Maersk, the Danish shipping conglomerate; at Merck, the American-based pharmaceutical giant; and even at businesses in Russia.

Attempted ransomware attacks against local governments in the United States have become unnervingly common. A 2016 survey of chief information officers for jurisdictions across the country found that obtaining ransom was the most common purpose of cyberattacks on a city or county government, accounting for nearly one-third of all attacks.

The survey, conducted by the International City/County Management Association and the University of Maryland, Baltimore County, also found that about one-quarter of local governments reported that they were experiencing attacks of one kind or another, successful or not, at least as often as once an hour.

Yet less than half of the local governments surveyed said they had developed a formal cybersecurity policy, and only 34 percent said they had a written strategy to recover from breaches.

Experts said government officials needed to be more aggressive about preventive measures, like training employees to spot and sidestep “phishing” attempts meant to trick them into opening the digital door for ransomware.

“It’s going to be even more important that local governments look for the no-cost/low-cost, but start considering cybersecurity on the same level as public safety,” said David Jordan, the chief information security officer for Arlington County, Va. “A smart local government will have fire, police and cybersecurity at the same level.”

Ms. Bottoms, who took office as mayor of Atlanta in January, acknowledged that shoring up the city’s digital defenses had not been a high priority before, but that now “it certainly has gone to the front of the line.”

“As elected officials, it’s often quite easy for us to focus on the things that people see, because at the end of the day, our residents are our customers,” Ms. Bottoms said. “But we have to really make sure that we continue to focus on the things that people can’t see, and digital infrastructure is very important.”

During the ransomware attack, local leaders have sometimes been able to do little but chuckle at a predicament that was forcing the city to turn the clock back decades.

Asked on Monday how long the city might be able to get by doing its business strictly with ink and paper, Ms. Bottoms replied: “It was a sustainable model until we got computer systems. It worked for many years. And for some of our younger employees, it will be a nice exercise in good penmanship.”

Security researchers trying to combat ransomware have noticed a pattern in SamSam’s attacks this year: Some of the biggest have occurred around the 20th of the month.

U.S. | A Cyberattack Hobbles Atlanta, and Security Experts Shudder

Allan Liska, a senior intelligence analyst at Recorded Future who has been tracking the group, said in an interview that he believed that SamSam gains access to its victims' systems and then waits for weeks before encrypting the victims' data. That delay, Mr. Liska said, makes it harder for responders to figure out how the group was able to break in — and easier for SamSam's hackers to strike twice.

The Colorado Department of Transportation was able to restore its systems on its own after a SamSam attack, without paying SamSam a dime. But a week later, the hackers struck the department again, with new, more potent ransomware.

"They are constantly learning from their mistakes, modifying their code and then launching the next round of attacks," Mr. Liska said.

Alan Blinder reported from Atlanta, and Nicole Perlroth from Boulder, Colo.

A version of this article appears in print on March 27, 2018, on Page A14 of the New York edition with the headline: Atlanta Hobbled by Major Cyberattack That Mayor Calls 'a Hostage Situation'

The Washington Post

National

8 days after cyberattack, Baltimore's network still hobbled

By David McFadden | AP
May 15 at 7:38 PM

BALTIMORE — More than a week after a cyberattack hobbled Baltimore's computer network, city officials said Wednesday they can't predict when its overall system will be up and running and continued to give only the broadest outlines of the problem.

Baltimore's government rushed to take down most computer servers on May 7 after its network was hit by ransomware. Functions like 911 and EMS dispatch systems weren't affected, officials say, but after eight days, online payments, billing systems and email are still down. Finance department employees can only accept checks or money orders.

No property transactions have been conducted since the attack, exasperating home sellers and real estate professionals in the city of over 600,000. Most major title insurance companies have even prohibited their agents from issuing policies for properties in Baltimore, according to the Greater Baltimore Board of Realtors.

Citing an ongoing criminal investigation, Baltimore's information technology boss Frank Johnson and other city leaders said Wednesday they could provide no specifics about the attack from the ransomware variant RobbinHood or realistically forecast when the various hobbled layers of the city's network would be back up.

"Anybody that's in this business will tell you that as you learn more those plans change by the minute. They are incredibly fluid," said Johnson, stressing that city employees, expert consultants and others were working "round the clock" to mend the breached network.

The FBI's cyber squad agents have been helping employees in Maryland's biggest city try to determine the source and extent of the latest attack.

Johnson's tenure has now included two major breaches to the city's computer systems. This month's problems come just over a year since another ransomware attack slammed Baltimore's 911 dispatch system, prompting a worrisome 17-hour shutdown of automated emergency dispatching. The March 2018 attack required operating the critical 911 service in manual mode.

Johnson is one of the city's highest paid employees, earning $250,000 a year. That's more than the mayor, the city's top prosecutor and the health commissioner are paid. This latest attack came about a week after the firing of a city employee who, the inspector general said, had downloaded thousands of sexually explicit images onto his work computer during working hours.

While all municipalities are menaced by malware, cybersecurity experts say organizations that fall victim to such attacks often haven't done a thorough job of patching systems regularly.

Asher DeMetz, lead security consultant for technology company Sungard Availability Services, suggested that eight days was a long time for a network to remain down.

"The City of Baltimore should have been prepared with a recovery strategy and been able to recover within much less time. That time would be dictated by a risk assessment guiding how long they can afford to be down," DeMetz said in an email. "They should have been ready, especially after the previous attack, to recover from ransomware."

City Solicitor Andre Davis said Baltimore was working "hand in glove" with the FBI, Microsoft officials, and expert contractors that he and other officials declined to identify. Before TV news crews, Davis likened the cyberattack to a brutal assault, a comparison that many residents can clearly understand in a city struggling to bring down one of urban America's highest rates of violent crime.

"My preferred way of thinking about it is: The city network was viciously assaulted by a culprit and seriously injured," Davis said. Baltimore's top lawyer portrayed the city network as an injured patient who has emerged from the ICU and faces a "long course of physical therapy."

Baltimore authorities, who hope to prosecute the culprit behind the latest attack, said they were in close contact with counterparts in Atlanta. Last year, a ransomware attack significantly disrupted city operations there and caused millions of dollars in losses. In December, two Iranian men already indicted in New Jersey in connection with a broad cybercrime and extortion scheme were indicted on federal charges in Georgia related to that ransomware attack demanding payment for a decryption key.

It's not clear what culprits are demanding from Baltimore's City Hall.

"We're not going to address or discuss in any way the ransom demand," Davis said.

___

Follow McFadden on Twitter: https://twitter.com/dmcfadd